IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 1:18-CR-22
	)	
Plaintiff	)	JUDGE: SOLOMON OLIVER, JR.
	)	
vs.	)	
	)	**DEFENDANT PHILLIP DURACHINSKY'S**
PHILLIP DURACHINSKY,	)	**REPLY BRIEF TO THE *GOVERNMENT'S***
	)	***RESPONSE IN OPPOSITION TO DEFENDANT'S***
Defendant	)	***MOTION TO SUPPRESS***

Now comes Defendant Phillip Durachinsky, by and through counsel, and replies to the *Government's Response in Opposition to Defendant's Motion to Suppress*. Notwithstanding the arguments made by the Government in their response brief, Defendant stands behind all of his factual assertions and legal arguments, including his supporting case law citations, which were set forth in his original Motion to Suppress Evidence and Statements. Further, Defendant contends that The Government has failed in its burden of proving that an applicable exception exists to the warrant requirement of the Fourth Amendment, which overcomes the per se Constitutional unreasonableness of the warrantless searches and seizure that occurred in the case at bar. Additionally, Defendant would like to specifically address the following erroneous statements of fact, and/or arguments of law, made by the Government:

1. The Government begins it brief in opposition by stating, "Durachinsky has confessed to the ultimate violation of privacy – infecting thousands of computers with a virus in order to secretly turn on the cameras and microphones on those computers so that Durachinsky could watch, record, and archive unwitting adults and children in a state of undress and/or engaged in sex acts". (Govt. Brief p.1). First, Defendant has seen

no evidence that "thousands" of computers were involved. In fact, Defendant has filed a motion for a bill of particulars demanding that the Government identify each specific computer that was infected. Secondly, Defendant adamantly denies that his purpose in viewing the remote camera video was to specifically view adults or non-adults in a state of undress or engaged in sex acts. Although less than a handful of teenagers, in various states of undress, happened to be recorded by the remote cameras, Defendant disputes that any of the teenagers were engaged in sex acts. Finally, Defendant's inculpatory proffer statements, which are not typical confession statements, are not accurately summarized by the Government's above-referenced statement. Moreover, the purported specific content of Defendant's proffer statements should not be used outside the parameters set forth in the proffer agreement.

2. Contrary to the Government's assertion at Govt. Brief p.8, Defendant adamantly denies using the Fruitfly malware to secretly "produce" child pornography and illicit images from unknowing children, or knowingly possessing such materials.
3. The Government concedes that by January 14, 2017, investigators knew for certain that the computer infections at issue in the case at bar (the Fruitfly malware) were connected to Defendant and Defendant's home address. Since the agents claim they made arrangements with a federal magistrate judge on January 18, 2017, prior to the search and seizure of Defendant's computer, to obtain a search warrant, the agents must have believed that they had that same requisite probable cause for the four days prior to making the arrangements with the magistrate judge. (See also Govt. Brief p.10). If the agents believed that they had probable cause to search

Defendant's home and seize and search his computer, prior to going to his home on January 18, 2017, why did they not apply for a search warrant during the four day period between January 14, 2017 and the warrantless search late at night on January 18, 2019.

4. The Government claims that two separate internet articles which appeared on June 18, 2017, and which referenced the malware that the Government is claiming that Defendant infected computers with, were the impetus for its effort to seize and search Defendant's computer later that date. The Government claims it was afraid that Defendant would read those articles and seek to evade detection, or destroy evidence. However, once again, since this was very important investigation, in which the identity of the suspect and location of the suspect's computer were well known, there was nothing preventing the Government from seeking and obtaining a search warrant, at any time during the above referenced four day period. Furthermore, investigators had absolutely no evidence that Defendant had read those articles, or was even aware of them.
5. The Government cites to Illinois v. McArthur, 531 U.S. 326 ((2001) in support of its "exigent circumstances" warrantless seizure of Defendant's laptop computer. However, McArthur held that where police had developed probable cause that illegal drugs were hidden inside a suspect's home, during a totally unrelated police matter at the suspect's home, it was reasonable to prevent the suspect from entering his own home while the police obtained a search warrant. Therefore, the officers' reactive actions at the scene were reasonable. This is not factually on point with what the investigators did in the case at bar. Moreover, the Government agents, in

the case at bar, could have done what the police did in McArthur, and prevented anyone, including Defendant, from gaining access to the laptop while they sought a warrant. Instead, they seized and searched the laptop without a warrant. It must also be emphasized that part of the exigent circumstances that the agents relied upon – evidence that Defendant was remotely accessing his computer, was obtained through the unlawful entering of Defendant's computer room and the unlawful opening of the laptop computer lid.

6. The Government mischaracterizes Defendant's argument regarding the unavailability of the exigence circumstance exception. Pursuant to the United States Supreme Court's holding in Kentucky v. King, 563 U.S. 452 (2011), "The exigent circumstances rule applies when the police do not create the exigency by engaging or threatening to engage in conduct that violates the Fourth Amendment." The Court went on to further state:

> The proper test follows from the principle that permits warrantless searches: warrantless searches are allowed when the circumstances make it reasonable, within the meaning of the Fourth Amendment, to dispense with the warrant requirement. Thus, a warrantless entry based on exigent circumstances is reasonable when the police did not create the exigency by engaging or threatening to engage in conduct violating the Fourth Amendment. A similar approach has been taken in other cases involving warrantless searches. For example, officers may seize evidence in plain view if they have not violated the Fourth Amendment in arriving at the spot from which the observation of the evidence is made, see Horton v. California, 496 U. S. 128, 136–140; and they may seek consent-based encounters if they are lawfully present in the place where the consensual encounter occurs, see INS v. Delgado, 466 U. S. 210, 217, n. 5. Pp. 8–10.
>
> (emphasis added)

In the case at bar, Defendant asserts that in order to view the laptop computer screen, that Government agents violated the Fourth Amendment in multiple ways, including but not limited to: (1) entering Defendant's computer room without consent, and moving a chair that was blocking the view of the laptop computer, and (2) opening the closed lid of the computer and looking at the screen; all done without Defendant's or his parents' consent. Therefore, the "exigent circumstances" exception to the warrant requirement is not available to the Government in this case.

7. The Government argues that even if the seizure of the Defendant's laptop was improper, since the law enforcement agents relied upon the Department of Justice attorneys, who presumably were supervising the investigation, they acted in good faith, and hence the exclusionary rule is not applicable. This is circular reasoning to the extreme. The Government is in effect arguing that since the Government agents relied on the Government attorneys, in violating the Constitution, the evidence that the Government agents seized for the benefit of the Government attorneys at trial, should not be excluded. Thus, the Government's reliance upon itself would excuse any improper conduct. This would not only fail to deter improper investigative actions, but would actually incentivize them. It is the unlawful searches by the Government, through its agents, that the exclusionary rule seeks to deter. Regardless of which Governmental "agent" was responsible (either the prosecutor or investigative agent) for making the decision to search and seize without a warrant, the exclusionary rule should be applied. The Government cites to Herring v. United States, 555 U.S.135 (2009), in support of its position. However Herring is not close to being on point. Herring involves good faith reliance upon a computer record

and/or a record clerk in determining that an individual had an outstanding warrant. In other words, there was a reliance by officers on a mistaken record that they were entirely justified in relying upon. It does not involve a deliberate decision by the investigating agents and prosecutors not to obtain a warrant in connection with the search of a home, search of an individual's personal room, search of an individual's computer, and the seizure of that computer. Similarly, Davis v. United States, 564 U.S. 229 (2011), was a good faith reliance by police on the current state of the law, that was subsequently changed by a later court decision. The other cases cited to by the Government involve split second reactive decision making by police officers in the heat of the moment. The case at bar involves a deliberate well thought out plan of action, in which investigators were in constant contact and collaboration with the prosecutors who would subsequently be prosecuting the case. They chose not to seek a search warrant, or arrest warrant for that matter, because either they believed that they did not have probable cause, prior to conducting the warrantless search of Defendant's home, or for some unknown tactical reasons.

8. The Government argues that the inevitable discovery doctrine applies, and emphasizes that the investigative agents had already arranged to seek a search warrant approval from a magistrate judge. However, the Sixth Circuit, in United States v. Griffin, 502 F.2d 959 (6th Cir. 1974), explicitly held the following:

> "We hold that absent any of the narrowly limited exceptions (See Katz v. United States, 389 U.S. 347, 357, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)) to the search warrant requirement, police who believe they have probable cause to search cannot enter a home without a warrant merely because they plan subsequently to get one. The assertion by police (after an illegal entry and after finding evidence of crime) that the discovery was 'inevitable' because

> they planned to get a search warrant and had sent an officer on such a mission, would as a practical matter be beyond judicial review. Any other view would tend in actual practice to emasculate the search warrant requirement of the Fourth Amendment.
>
> (Emphasis added)

Further, in United States v. Buchanan, 904 F.2d 349 (6th Cir. 1990), the Court, in rejecting the applicability of the inevitable discovery doctrine, reasoned as follows:

> We reject the government's argument for application of the inevitable discovery exception. The agents in this case were not pursuing an alternate line of investigation of Buchanan. The agents were sent to observe the Buchanan residence in order to develop probable cause for a search warrant, and if they developed probable cause, it was only through interrogation of Buchanan. However, prior to initiating the warrant application for the Buchanan residence, the agents made an illegal entry into the home which "tainted the only ... investigation that was ongoing." United States v. Owens, 782 F.2d 146, 152 (10th Cir.1986).

As the Government will acknowledge, at the time of warrantless search and seizure at the Defendant's home, agents were using an investigative technique referred to in the FBI 302 report as a "knock and talk". This was a phase of the only investigation of Defendant that was taking place, and it was tainted by the unlawful searches and seizure that took place at the Defendant's home.

CONCLUSION

Defendant respectfully requests that the Court find that Defendant's personal laptop computer, the computer data found on Defendant's personal computer, work computer, and external drives/flash drives, as well as his two proffers statements be

suppressed as having been obtained in violation of his Fourth Amendment rights. Any and all other evidence obtained as a result of Defendant's proffer statements, or derivatively obtained from any of the aforementioned computer data must also be suppressed.

Respectfully submitted,

/s/ Thomas E. Conway
Thomas E. Conway (Reg. 0021183)
Attorney for Defendant
55 Public Square Suite 2100
Cleveland, Ohio 44113
(216) 210-0470 - phone
(216) 621-8714 - Fax
teconway@sbcglobal.net - Email

CERTIFICATE OF SERVICE

I certify that the forgoing was filed electronically on May 19, 2019. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system, and can be accessed through said system.

/s/ Thomas E. Conway
Thomas E. Conway